AOS-W 6.5.1.0

Alcatel·Lucent
Enterprise

Release Notes

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents 3

Revision History 5

Release Overview 6

Chapter Overview 6

Supported Browsers 6

Contacting Support 7

New Features 8

Regulatory Updates 20

Resolved Issues 21

Known Issues 45

Upgrade Procedure 61

Upgrade Caveats 61

GRE Tunnel-Type Requirements 62

Important Points to Remember and Best Practices 62

Memory Requirements 63

Backing up Critical Data 64

Upgrading in a Multiswitch Network 65

Installing the FIPS Version of AOS-W 6.5.1.0 65

Upgrading to AOS-W 6.5.1.0 66

Downgrading 69

Before You Call Technical Support 71

Acronyms and Abbreviations 72

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W 6.5.1.0 is a software release that includes new features and enhancements introduced in this release and fixes to issues identified in previous releases.

NOTE

See the Upgrade Procedure on page 61 for instructions on how to upgrade your switch to this release.

Chapter Overview

- New Features provides a description of features and enhancements introduced in this release.
- Regulatory Updates describes the regulatory updates in this release.
- Resolved Issues describes the issues resolved in this release.
- Known Issues describes the known and outstanding issues identified in this release.
- Upgrade Procedure describes the procedures for upgrading a switch to this release.

NOTE

For information regarding prior releases, refer to the corresponding Release Notes on https://service.esd.alcatel-lucent.com/.

Supported Browsers

The following browsers are officially supported for use with AOS-W 6.5.1.0 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS
- Chrome 51.0.2704.103 m (64-bit)
- Microsoft Edge 25.10586.0.0 and Microsoft Edge HTML 13.10586

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	http://enterprise.alcatel-lucent.com
Support Site	https://support.esd.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This section describes the new features, enhancements, and hardware introduced in AOS-W 6.5.1.0. For more information about these features, refer to the *AOS-W 6.5.1.0 User Guide*.

Security Update

Support for SHA2 Signature for Image Verification

The switch images now support SHA2 signature for image verification. While copying new images to the switches, both SHA1 and SHA2 signatures are validated.

Revocation of AOS-W Default Certificate Issued by GeoTrust

The switch-issued server certificate replaces the AOS-W default certificate issued by **GeoTrust Public CA** for WebUI authentication, Captive Portal, 802.1X termination, and Single Sign-On (SSO) because the default certificate is now revoked.

For more information on the **GeoTrust Public CA** certificate revocation, refer to the advisory.

Using the switch-issued server certificate has the following caveats:

- When MacBook or iOS devices connect to Captive Portal, the CNA (Captive Network Assistant) pop-up does not appear. So, you must open a browser to get redirected to a Captive Portal page.
- When the Captive Portal custom welcome page is configured in Mac Safari 8.1, the certificate warning pops up as soon as the welcome page appears.
- WISPr authentication fails on the switch.
- Authentication Survivability fails on Windows clients using EAP-TLS authentication.
- 802.1X PEAP authentication fails on Windows 7 clients. So, you must disable the **Validate Server Certificate** option on the Windows 7 clients.

NOTE

It is recommended to use custom certificates to avoid these caveats.

OV3600 Management

Clarity Synthetic Enhancements

Starting from AOS-W 6.5.1.0, Clarity Synthetic is supported in the following AP platforms:

- OAW-AP207 access point

- OAW-AP300 Series access points
- OAW-AP310 Series access points
- OAW-AP320 Series access points
- OAW-AP330 Series access points

ARM

Traffic Steering

ARM’s traffic steering feature encourages clients that support both Wi-Fi and 3G/4G cellular connections to move from a Wi-Fi connection to a cellular connection when the device moves out of a Wi-Fi coverage area, or when the Wi-Fi connection supports lower data rates than the cellular connection.

Wi-Fi and 3G/4G-compatible devices can be steered to a different connection type based upon the signal-to-noise ratio seen by clients attempting to associate to the network. If the cellular switch determines that the device's WLAN connection throughput has fallen below a determined threshold, the cellular switch tells the WLAN switch to disassociate the device from the network, and prevents neighboring APs from responding to the client's probe requests for a customizable blackout interval, preventing the client from reassociating to the Wi-Fi network. This blackout time is defined using the **RTTS-Backoff** VSA attribute in the RTTS Access Accept message. Use the traffic steering feature in deployments where a single operator provides both Wi-Fi and cellular network, and the user onboarding and accounting for both network types is managed by a common RADIUS server. This feature is disabled by default, and must be enabled for each SSID via the WLAN SSID profile. This feature requires that client match is enabled in the ARM profile used by your access points. (Client Match is enabled by default.)

AP-Platform

Support for OAW-AP207 Access Point

OAW-AP207 wireless access point supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with a dual 2x2 radio. Multiple-Input Multiple-Output (MIMO) technology allows the AP to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. OAW-AP207 wireless access point works in conjunction with a switch.

OAW-AP207 wireless access point provides the following capabilities:

- Wireless transceiver
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af Power over Ethernet (PoE)
- Centralized management configuration and upgrade
- Integrated Bluetooth Low Energy (BLE) radio
- Mesh support

For more information, see the *OAW-AP207 Wireless Access Point Installation Guide*.

Support for OAW-AP300 Series Access Point

The OAW-AP300 Series (OAW-AP304 and OAW-AP305) wireless access points support IEEE 802.11ac standards for high-performance WLAN, and are equipped with a dual 2x2 radio on 2.4 GHz and 3x3 radio on 5 GHz, which provide network access and monitor the network simultaneously. These APs deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The OAW-AP300 Series wireless access points work in conjunction with a switch.

The OAW-AP300 Series wireless access points provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatible with IEEE 802.3af PoE and IEEE 802.3at PoE+
- Centralized management configuration and upgrade
- Integrated BLE radio

For more information, see the *OAW-AP300 Series Wireless Access Point Installation Guide*.

3G and 4G USB Modem Support on OAW-AP300 Series Access Points

AOS-W 6.5.1.0 introduces the support for the following USB modems on OAW-AP300 Series access points:

- Huawei E3372 (Huawei)
- Netgear AirCard 340U (AT&T)
- Netgear AirCard 341U (Srpint)
- Franklin Wireless U770 (Sprint)
- Pantech UML290 (Verizon)
- Pantech UML295 (Verizon)
- Novatel MC551L (Verizon)
- Novatel U620L (Verizon)

Alcatel One Touch L800 4G LTE Modem Support

AOS-W 6.5.1.0 introduces the support for the Alcatel One Touch L800 4G LTE USB modem on OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points.

Mesh Support for OAW-AP310 Series and OAW-AP320 Series Access Points

Starting from AOS-W 6.5.1.0, mesh support is introduced for OAW-AP310 Series access points (OAW-AP314 and OAW-AP315) and OAW-AP320 Series access points (OAW-AP324 and OAW-AP325).

Support for The APM-210

AOS-W 6.5.1.0 introduces the support for the APM-210, a high-performance dual-radio 3x3:3 MIMO 802.11ac wireless Access Point Module (APM). This product enhances the Ericsson Pico Radio Base Station by enabling Wi-Fi access as an add-on to indoor WCDMA or 3GPP cellular coverage.

Frame-Drop Counter Messages

AOS-W 6.5.1.0 uses AMON messages to report data collected by an AP's WMM frame-drop collectors. This system sends messages that allow clients to monitor individual queues as they are sent/received by the AP.

MAC Address Filter

AOS-W 6.5.1.0 enables APs to filter randomized MAC addresses before compiling the list of unassociated devices that are reported in the RSSI feed.

Active Number of MU-MIMO Groups

Starting from AOS-W 6.5.1.0, a new parameter, **mu-status ap-name <ap-name>**, is introduced in the **Show AP debug** command to view the active number of MU-MIMO groups formed and the state per group information.

Support for OCSP and USB Custom Certificate on OAW-AP205H

Starting from AOS-W 6.5.1.0, support for Online Certificate Status Protocol (OCSP) and USB custom certificate is introduced on OAW-AP205H remote access points. With this feature:

- OAW-AP205H remote access points support checking the revocation status of the switch certificate by reading the AIA field of the server certificate with its corresponding OCSP responder.
- OAW-AP205H remote access points can store CSR and private key files and read the custom certificate stored in .p12 certificate format for establishing IKE/IPSEC tunnel with a switch.

AP Datapath

AP LACP Limitation

AP LACP is not supported for remote and mesh OAW-AP324/OAW-AP325 access points.

Base OS Security

Customizing the RADIUS Attributes

The users can configure RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server. The RADIUS modifier profile can be configured and applied to either Access- Request or Accounting-Request or both on a RADIUS authentication server.

Branch Switches

WAN Optimization through IP Payload Compression

AOS-W 6.5.1.0 introduces the support for WAN optimization through IP payload compression in OAW-4450 switches.

Support for Jumbo Frames

Starting from AOS-W 6.5.1.0, use the branch office switch Smart Config feature to enable or disable jumbo Ethernet frames on branch office switch ports.

Allow US Territory on US SKU Switch

AOS-W 6.5.1.0 introduces the capability for US SKU switch to accept all the US territory APs in addition to US APs. The list of US territories allowed on the US SKU switch are:

- Puerto Rico
- Guam,
- US Virgin Islands
- Northern Mariana Islands
- American Samoa
- Federated States of Micronesia
- Marshall Islands

USB Modem Support on OAW-40xx Series Switches

AOS-W 6.5.1.0 introduces the support for the following USB modems on OAW-40xx Series switches:

- Huawei E3276-150 (Huawei)
- Huawei E3372-153 (Huawei
- Netgear 320U (AT&T))

Support for SFP-ZX Modules

AOS-W 6.5.1.0 introduces support for SFP-ZX Modules on the following switches:

- OAW-4010
- OAW-4024
- OAW-4030
- OAW-4x50 Series

Alcatel-Lucent supports the SFP-ZX modules with the following specification:

- Transceiver Type : CWDM
- Data Rate: 1.25 Gb/s
- Wavelength: 1530 nm, 1590 nm, 1390 nm, and 1470 nm
- Fiber Type: Single -mode fiber
- Max Distance: 80 kms and 120 kms
- Optical Components: DFB/PIN
- Connector: Duplex LC

Support for New SFP, SFP+ and DACs

AOS-W 6.5.1.0 introduces support for the following SFP, SFP+, and DACs :

- The following SFP modules are supported in OAW-4010, OAW-4024, OAW-4030, and OAW-4x50 Series switches:
  - J4858C HPE X121 1G SFP LC SX Transceiver
  - J4859C HPE X121 1G SFP LC LX Transceiver
  - J8177C HPE X121 1G SFP RJ45 T Transceiver
- The following SFP+ modules are supported in OAW-4024 and OAW-4x50 Series switches:
  - J9150A HPE X132 10G SFP+ LC SR Transceiver
  - J9151A HPE X132 10G SFP+ LC LR Transceiver
  - J9153A HPE X132 10G SFP+ LC ER Transceiver
- The following DACs are supported in OAW-4024 and OAW-4x50 Series switches:
  - J9281B HP X242 10G SFP+ SFP+ 1m DAC Cable
  - J9283B HP X242 10G SFP+ SFP+ 3m DAC Cable
  - J9285B HP X242 10G SFP+ SFP+ 7m DAC Cable

DHCP

Customization of DHCP Relay Agent Information Option (Option-82)

Option-82 can now be customized to cater to the requirements of any Internet Service Provider (ISP) using the Alcatel-Lucent switch. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option-82 have been introduced.

High Availability

High Availability on the Backup LMS

Starting with AOS-W 6.5.1.0, high availability is supported on the backup LMS. When an LMS and backup LMS are migrated to the high availability redundancy solution with the **dual**switch role:

- Each switch has its own standby (backup) switch.
- Newly deployed APs can connect directly to each switch in active mode.
- APs can failover to a backup switch in standby mode when their primary switch becomes unavailable. The backup switch then becomes the active switch for these APs.
- LMS preemption is disabled. Under LMS preemption, APs automatically reconnect to the LMS as soon as it comes back up. Under the high availability solution, APs remain connected to an active backup switch until it becomes unavailable. When the backup switch fails, the APs failover to the backup's standby switch, which can be the AP's primary switch or another switch.

High Availability Alerting

Starting from AOS-W 6.5.1.0, new Management Information Bases (MIBs) are introduced to enable the switch provide the high availability status information to customers.

The following are the new MIBs introduced in AOS-W 6.5.1.0 for High Availability Alerting:

- High Avalability Config Table: *wlsxHighAvalabilityConfigTable*—provides HA enabled/disabled status, HA group membership, and parameters configured in HA group profile.
- HA AP Table: *wlsxHighAvalabilityApTable*—provides Active APs count, Standby APs count, and Total APs count.
- Interswitch Heartbeat Table: *wlsxIntercontrollerHbtTable*—provides Active switch IPs, Reference count, and heartbeat statistics for each active switch.
- HA State Sync Table: *wlsxStateSyncTable*—provides active/replicated/total PMK cache entries and key cache entries count.
- HA Tunnel Table: *wlsxHighAvalabilityTunnelTable*—provides active/standby/total BSS tunnel count and total heartbeat tunnel count.

All the MIBs for the HA Alerting feature are implemented in *wlsxHaMIB*.

The new SNMP traps introduced for High Availability Alerting in AOS-W 6.5.1.0 are as follows:

- HA State trap: *wlsxHaState*—indicates that HA state has changed.
- Standby IP Sent Failed Trap: *wlsxHaStandbyIpSentFailed*—indicates that standby IP is sent to an AP failed.
- HA Standby Connectivity State Trap: *wlsxHaStandbyConnectivityState*—indicates the standby connectivity status for an AP.
- HA Interswitch Hbt Miss Trap: *wlsxHaIntercontrollerHbtMiss*—indicates that around half of the threshold interswitch heartbeat was missed with serving switch.
- HA Failover Trigger Trap: *wlsxHaFailoverTrigger*—indicates that standby switch has triggered HA failover to APs belonging to a particular serving switch with which interswitch heart beat was missed above threshold.

- HA Failover Request from AP Trap: *wlsxHaFailoverRequestFromAp*—indicates that an AP sent failover request to the switch. This could be because of AP missing heartbeat with the serving switch, and on receiving failover request from standby switch or AP trying to preempt back to active switch

For more information on the MIBs, OIDs and SNMP traps, refer to the *aruba-ha.my* MIB file, which is available within *aruba-mibs_6.5.1.0_56684.tar.gz* in the **Download Software** tab of support.arubanetworks.com.

Hotspot 2.0 Enhancements

The Hotspot feature includes a new Hotspot 2.0 Query Protocol (H2QP) **OSU provider list** profile that defines the list of Online Sign-Up (OSU) providers to be sent in the ANQP IE. If a customer device cannot automatically complete 802.1X authentication with the operator of the hotspot or any of its roaming partners, the device receives a notification from the hotspot that additional Online Signup services are available.

The Hotspot 2.0 profile is enhanced to support a service provider's network QoS by mapping the service provider's Layer-3 QoS priorities (defined via DHCP) to an over-the-air Layer 2 priority. This feature is designed to optimize the user experience for clients using devices that move between cellular and Wi-Fi networks. The Hotspot 2.0 profile also allows network administrators to specify if the hotspot uses a a OSU Server-only authenticated layer 2 Encryption Network (OSEN) network type. This hotspot type can provision clients using an Open ESS or a OSEN WLAN.

IPsec

Provision to Configure MTU for Virtual Adapter

AOS-W VIA calculates optimal MTU value for the virtual adapter based on the physical network interface on the client machine. But in some situations, this optimal value may not be desired. This feature allows the administrator to change the MTU value used by VIA. This feature can be configured using the **VIA Client mtu value** parameter introduced in AOS-W 6.5.1.0.

For more information, refer to the *Alcatel-Lucent AOS-W VIA 2.3.4 Windows® Edition.Release Notes*.

IPv6

IPv6 Router Advertisement Proxy

Whenever a new client joins the network, a unicast or a multicast Router Advertisements (RA) is sent to from the router to the client. If it is a multicast packet then existing clients also receive the RA, which results in increasing the traffic. Starting from AOS-W 6.5.1.0, this issue is addressed by enabling IPv6 proxy RA to snoop incoming unsolicited Router Advertisement and Router Solicitations packets.

Licensing

Changes to WebCC Subscription License Management

Starting with AOS-W 6.5.1.0, if one or more subscription WebCC licenses expire so that a switch has fewer active WebCC subscription licenses than AP licenses, that switch will no longer be able to download WebCC updates from the cloud. The APs associated to that device, can, however, continue to use the cached WebCC date currently on the switch. This is a change from AOS-W 6.5.0, where an expired WebCC license did not impact AP or switch behavior.

Logging

Support for CEF Logging

Starting from AOS-W 6.5.1.0, support for Common Event Format (CEF) logging is introduced for switches. The ArcSight CEF is a log management standard that uses a standardized logging format so that data can easily be collected and aggregated for analysis by an enterprise management system.

Support for RFC 3164 Logging

Starting from AOS-W 6.5.1.0, RFC 3164 or BSD standard format logging can be configured through the CLI and WebUI.

Ping

Ping Enhancements

The following Ping options are introduced:

- Interval
- Pattern
- Timeout
- ToS
- TTL
- Validate-Reply

QoS Enhancements

AOS-W 6.5.1.0 introduces the following enhanced traffic QoS features.

QoS for AP Management Traffic:

Management traffic on the AP can now be marked with Differentiated Service Code Point (DSCP) values to apply a priority level to that traffic. The **Management DSCP** field is introduced in the AP system profile to support this feature.

DSCP to 802.1P mapping:

The AP system profile allows a user to map IP DSCP priorities (0-63) to a 802.1p priority level (0-7) at the AP's media access control (MAC) level. The **IP DSCP to VLAN 802.1P priority mapping** field is introduced in the AP system profile to support this feature.

QoS for EAP Auth Traffic

Extensible Authentication Protocol (EAP) traffic can be assigned to a specific Wi-Fi Multimedia (WMM) traffic class. By default, EAP traffic is mapped to the "best effort" traffic class. The **WMM Access Class of EAP traffic** field is introduced in the SSID profile to support this feature.

RADIUS

RADIUS VSA Enhancements

The following new RADIUS Vendor-Specific Attributes (VSA) are introduced to support the new traffic steering feature.

- **RTTS-Estimated-Throughput:** Used to transfer a UE through-put estimation value from a RADIUS authenticator to the CWC (via a RADIUS proxy).
- **RTTS-Result**: Used by the CWC to transfer the result of a traffic steering decision to the RADIUS authenticator.
- **RTTS-Backoff-Time**: Used by the CWC in the Access-Accept packet to indicate to the WLAN how long a rejected UE should be ignored before being considered again for entry into the WLAN.
- **RTTS-Reestimation-Period**: Included by the CWC in the Access-Accept packet when RTTS-Result is True to indicate to the WLAN the required interval of time between RTTS Throughput estimates to be sent to the CWC for the UE.
- **RTTS-Reest-Below-Throughput** : Included by the CWC in the Access-Accept packet when RTTS-Result is True to indicate to the WLAN the level below which RTTS Accounting-Request packets should be sent.
- **RTTS-Reest-Keepalive-Num** :This attribute is included by the CWC when RTTS-Result is True in order to ensure that not too many reestimations are skipped by the WLAN due to the UE Wi-Fi estimated throughput being constantly higher than the RTTS-Reestimate-When-Below-Tput threshold.
- **RTTS-Earlylift-Threshold**:Included by the CWC when RTTS-Result is False to indicate to the WLAN a minimum UE throughput level at which it is worthwhile interrupting the Backoff Timer to allow the UE to try and access the WLAN again. If the UE throughput is above this level, it is highly likely the UE will be accepted to Wi-Fi during the subsequent RTTS comparison. The purpose of this attribute is to not unduly block a UE whose Wi-Fi RF conditions have dramatically improved.

The following new RADIUS VSAs are introduced to support Hotspot 2.0 feature enhancements.

- **Hotspot2-Subscription-Remediation-URL**: Defines the provisioning supported by the subscription remediation server and a Subscription Server URL sent to a client that is unable to authenticate using its existing credentials.
- **Hotspot2-AP-Version**: Indicates the Hotspot release version supported by the AP. Supported values are **0** for Release 1, and **1** for Release 2.
- **Hotspot2-STA-Version**: Indicates the Hotspot release version supported by the mobile device. Supported values are **0** for Release 1, and **1** for Release 2.
- **Hotspot2-Deauthentication-Request**: Use this VSA to specify the reason the mobile device is being de-authenticated, define the delay time (in seconds) that a mobile device waits before attempting re-association to the same BSS, and define theURL of a server that explains why the mobile device was not authorized.

- **Hotspot2-Session-Info-URL**: Send a BSS Transition Management Request frame before the mobile device's session is terminated, warning the user their session is about to end. Specify a URL in this VSA to provide a link to a webpage that provides the user with information on how to extend their session.

Server Load Balancing for RADIUS Accounting

The AOS-W switches perform load balancing of RADIUS accounting packets that are destined to external RADIUS Servers to ensure accounting load gets distributed.

RADIUS Server Response Enhancement

Starting from AOS-W 6.5.1.0, the **aaa test-server** command includes a new **verbose** option that will display the RADIUS server's response on a successful or failed authentication.

This enhancement applies to both the WebUI and the CLI.

Roles

Standard Role

Starting from AOS-W 6.5.1.0, a new management role, Standard role, is supported which has all the root privileges but cannot make changes to the management users. The purpose of creating this new role is to prevent changes to the local account from externally authenticated management user.

Security

Null Encryption

Starting from AOS-W 6.5.1.0, XLP based switches are supported with null encryption for IKEv1 as an encryption algorithm. This helps in reducing the load on the local router for internet destined traffic.

ANY-ANY Crypto Map

Starting from AOS-W 6.5.1.0, any-any selectors are negotiated in IKEv1 to enable the option of having numerous tunnels. After pre-connect flag is enabled for IPsec map, IKE triggers the tunnel to the peer ip and proposes any-any traffic selector.

PAPI Enhanced Security

Starting from AOS-W 6.5.1.0, a minor security enhancement is made to Process Application Programming Interface (PAPI) messages. With this enhancement, PAPI endpoints authenticate the sender by performing a sanity check of the incoming messages using MD5 (hash).

All PAPI endpoints—access points, Mobility Access Switches, switches, Analytics and Location Engine (ALE), OV3600, and HPE switches—must use the same secret key.

The PAPI Enhanced Security configuration provides protection to Alcatel-Lucent devices, OV3600, and ALE against malicious users sending fake messages that results in security challenges.

You can configure the PAPI Enhanced Security feature from either the WebUI or the CLI.

Authentication Survivability

The **Cache Lifetime** parameter value in Authentication Survivability is increased from 72 hrs to 168 hrs.

Chapter 3
Regulatory Updates

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

Regulatory Updates in AOS-W 6.5.1.0

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.1.0:

- DRT-1.0_56643

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at service.esd.alcatel-lucent.com.

NOTE

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the service.esd.alcatel-lucent.com site.

Chapter 4
Resolved Issues

This section describes the issues resolved in AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
103991 105074 105212 105628 106467 108995 110880 111201 113192	**Symptom:** A multicast video stream failed to respond on Windows Media Player clients. The fix ensures that multicast video stream is continuous on Windows Media Player clients **Scenario:** This issue occurred when the number of clients on an AP exceeded 20. This issue was observed in switches running AOS-W 6.4.0.2.	AP-Wireless	All platforms	AOS-W 6.4.0.2	AOS-W 6.5.1.0
113765 141672	**Symptom:** When a user issued the command to delete SNMP trap hosts these entries were not getting deleted on the switch. This issue is resolved by adding a check to ensure that the same user is not referenced to different targets. **Scenario:** This issue occurred when the same user was configured for different targets and the entire list was deleted. When one host was deleted, the CLI also deleted the user parameters. Subsequent deletes did not locate the user, thereby resulted in the SNMP trap hosts not being deleted.	SNMP	All platforms	AOS-W 6.4.3.0	AOS-W 6.5.1.0
118685	**Symptom:** OAW-AP175 access points rebooted. This issue is resolved by adding a memory monitor to identify the location of memory leakage. **Scenario:** This issue occurred because of a memory leakage in the OAW-AP175 access points running AOS-W 6.3.1.15.	AP-Wireless	OAW-AP175 access points	AOS-W 6.3.1.15	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
119293	**Symptom:** The switch failed to prioritize traffic based on the Wi-Fi Multimedia (WMM) traffic management profile. The fix ensures that the switch prioritizes WMM traffic. **Scenario:** The throughput bandwidth share across voice, video, best effort, and background was different from the bandwidth share configured in the WMM traffic management profile. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.0 or later versions.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.0	AOS-W 6.5.1.0
123819	**Symptom:** ANQP response does not contain operator-friendly name when language code is set to anything except eng. This issue is resolved by adding validation to prevent incorrect configuration. **Scenario:** This issue was observed when the Hotspot operator \-friendly name was a non-english value. This issue was observed in OAW-AP200 Series access points running AOS-W 6.4.4.0.	Hotspot-11u	OAW-AP200 Series access points	AOS-W 6.4.4.0	AOS-W 6.5.1.0
126616 145721	**Symptom:** Wired users failed to pass traffic due to incorrect VLAN mapping. The fix ensures that the clients are assigned with correct VLANs to avoid this issue. **Scenario:**This issue occurred when a RAP was disconnected from the switch during a RAP backup process. This issue was observed in APs operating as RAPs.	AP-Datapath	All AP platforms	AOS-W 6.3.1.9	AOS-W 6.5.1.0
127853	**Symptom:** A switch generated continuous loop syslog entry every 3 to10 seconds, and over time, the APs stopped accepting configuration updates and failed to function correctly. This issue is resolved by altering the validation so that an invalid icon name is not accepted and by displaying an error message as soon as an invalid icon name is entered. **Scenario:** This issue occurred when an invalid icon file name was accepted at Hotspot OSU provider list profile level. This issue was observed in OAW-40xx Series switches running AOS-W 6.4.4.0.	Hotspot-11u	OAW-40xx Series switches	AOS-W 6.4.4.0	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128209	**Symptom:** When a user tried to hard reboot a switch, it failed to reboot with the following error: **not enough space on flash** The fix ensures that the flash backup excludes unwanted data to avoid database file corruption. **Scenario:** This issue occurred occasionally due to a database file corruption. This issue was observed in switches running AOS-W 6.4.2.x or later versions.	Switch-Platform	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.1.0
129692 138741	**Symptom:** In a master-standby-master setup, access points rebooted when the master failed. The fix ensures that HA is functional when access points rebootstrap to the Backup Local Mobility Switch (BLMS). **Scenario:** Access points were unable to setup a standby tunnel with the Local Mobility Switch (LMS), if the LMS was not reachable when the access points attempted to connect for the first time. This issue was observed in OAW-4550 switches running AOS-W 6.4.3.5.	AP-Platform	OAW-4550 switches	AOS-W 6.4.3.5	AOS-W 6.5.1.0
130983 136014 141304	**Symptom:** The PBR configuration in a standby switch was not retained after saving and reloading the standby switch. The fix ensures that the local PBR configuration is updated to handle cfg cleanup and forward referencing after a cfg synchronization is complete. **Scenario:** This issue was observed in standby switches running AOS-W 6.4.3.7 in a master-standby topology.	Policy Based Routing	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
131511	**Symptom:** A Simple Network Management Protocol (SNMP) server did not receive SNMP traps from a switch when a Link Aggregation Control Protocol (LACP) link failed. The fix ensures that an SNMP server receives SNMP traps from the switch. **Scenario:** This issue occurred because of a delay in electing a member in an LACP interface when one member failed. This issue was observed in switches running AOS-W 6.4.3.4.	SNMP	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.1.0
132230	**Symptom:** An SNMP server timed out the connection with a switch randomly. The fix ensures that the SNMP server is independent of the MODEM reinitialization. **Scenario:** This issue occurred because a MODEM connected to a switch was in standby mode and reinitialized every 2 minutes. This issue was observed in OAW-40xx Series switches running AOS-W 6.4.2.5 or AOS-W 6.4.2.12.	SNMP	OAW-40xx Series switches	AOS-W 6.4.2.5	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132239 134538 148386 148387 148388 148389 148390	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Aruba watchdog bark interrupt received on core 0**. This issue is avoiding socket buffer double free situations. **Scenario:** This issue occurred because of socket buffer double free situation. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.3.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.3	AOS-W 6.5.1.0
134394 146970	**Symptom:** After the AP was rebooted, the AP configuration was lost, so the AP could not terminate on the switch. This issue is resolved by adding a mechanism to recover the apboot environment if it is lost. If apboot environment is lost, the AP will recover the environment configuration and then reboot. **Scenario:** This issue is observed when the AP power is frequently turned off and on. This issue was observed in OAW-AP104 and OAW-AP105 access points running AOS-W 6.4.0.3.	AP-Platform	OAW-AP104 and OAW-AP105 access points	AOS-W 6.4.0.3	AOS-W 6.5.1.0
134719	**Symptom:** AP sent the same TX power decrease request repeatedly to the process on the switch that handled AP management and user association, until the request was accepted. This issue is resolved by downloading the FW and ACL configuration only when there is VAP related configuration change. **Scenario:** This issue was observed when the power setting in the ARM profile of a switch was changed. This issue was observed in switches running AOS-W 6.5.0.0.	ARM	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.1.0
136109	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by avoiding memory corruption. **Scenario:** This issue occurred because of memory corruption. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Datapath	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
137031	**Symptom:** Clients were unable to associate to the 2.4 GHz radio of OAW-AP225 access points intermittently. This issue is resolved by resetting the striping IP when an AP fails over to backup LMS or preempts back to main LMS. **Scenario:** SAP LACP striping IP was configured on the AP's backup LMS and not on the primary LMS. When an AP failed over to the backup LMS and preempted back to the primary LMS, it retained the striping IP provided by the backup LMS and continued to send traffic on the 2.4 GHz radio to the backup LMS. The local switch dropped this traffic because the Virtual AP profiles were not registered. This issue was observed in OAW-AP225 access points running AOS-W 6.4.3.4.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.3.4	AOS-W 6.5.1.0
137339 145475	**Symptom:** Port-channel links were not visible in the NMS tool (OV server). This issue is resolved by adding port-channel interface details. **Scenario:** This issue occurred when the switch did not return the port-channel interfaces. This issue was observed in switches running AOS-W 6.4.3.4.	SNMP	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.1.0
138093	**Symptom:** The **station management** (STM) process crashed multiple times in the switch. The fix ensures that the process does not crash. **Scenario:** The backup LMS failed to handle a large number of AP fallback. The switch ran out of memory and failed to restart the **STM** process. This issue was observed in switches running AOS-W 6.4.2.x and AOS-W 6.5.x.	Station Management	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.1.0
138320	**Symptom:** A wired user role did not change when the client moved from one VLAN to another. This issue is fixed by prioritizing the initial role over the derived role. **Scenario:** This issue occurred when the wired client was passing through a switch connected to a switch over an untrusted port . This issue was observed in switches running AOS-W 6.4.3.2.	Roles/VLAN Derivation	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138647	**Symptom:** A system-defined net-destination VRRP IP address did not handle multiple VRRP IP addresses. This issue is resolved by saving multiple VRRP IP addresses as a list in net-destination and handling modify messages appropriately. **Scenario:** This issue occurred because a system-defined net-destination stored only a single VRRP IP address and did not handle modification of VRRP IP address. Hence, when more than one VRRP IP address was configured, the ACL filters were not created for any VRRP IP address. This issue was observed in switches running AOS-W 6.3.1.18.	Switch-Platform	All platforms	AOS-W 6.3.1.18	AOS-W 6.5.1.0
139189 147270 147641 150011	**Symptom:** An AP crashed and the log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is resolved by limiting the number of broadcasts and at the same time reserving some space for these broadcasts on the queue. **Scenario:** This issue occurred when multiple virtual access points were used in the bridge mode. This issue was observed in OAW-AP225 access points running AOS-W 6.5.0.0.	AP-Platform	OAW-AP225 access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0
139192	**Symptom:** A RAP with a 340U MODEM for cellular uplink failed to boot. This issue is resolved by applying a script on 340U modems that do not have a LINUX patch. **Scenario:** This issue was observed in remote access points running AOS-W 6.5.0.0 and using 340U MODEM for cellular uplink.	Remote Access Point	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.1.0
139231	**Symptom:** OAW-AP330 Series access points working in AM mode with VHT disabled failed to find APs or clients on Radio a. This issue is resolved by overriding **VHT_enable** when in AM mode, so that the VHT always remains enabled. **Scenario:** This issue occurred when VHT was disabled in the AP's Radio a. This issue was observed in OAW-AP320 Series and OAW-AP330 Series access points running AOS-W 6.5.0.0.	AP-Wireless	OAW-AP320 Series and OAW-AP330 Series access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139340 144313 144591	**Symptom:** A client that was connected to a wireless bridge did not get an IP address from a DHCP server. This issue is resolved by adding an indirect MAC entry for all clients behind a wireless bridge and sending DHCP packets over all tunnels in a VLAN if broadcast-filter-arp is disabled. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
139424	**Symptom:** OAW-AP320 Series access points falsely detected a RADAR event and changed the channel on the radio. The fix ensures that a false RADAR event is not detected in the European Telecommunications Standards Institute (ETSI) domain and the AP works as expected. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.5.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.5	AOS-W 6.5.1.0
139799	**Symptom:** The AirGroup CPPM server table was not populated if FQDN was configured instead of an IP address in RADIUS authentication server profile. This issue is fixed by having checks in the response code to ensure that the AirGroup CPPM server is populated. **Scenario:** This issue occurred because of a memory leak. This issue was observed in switches running AOS-W 6.4.3.4.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.1.0
140007	**Symptom:** IPv6 Virtual Router Redundancy Protocol (VRRP) was not functional on an untrusted VLAN or port. This issue is resolved by adding support for IPv6 VRRP on an untrusted VLAN or port. **Scenario:** This issue is observed when VRRP advertisement without IPsec is sent over a VLAN or untrusted port. This issue was observed in OAW-4750 switches running AOS-W 6.4.4.5.	Base OS Security	OAW-4750 switches	AOS-W 6.4.4.5	AOS-W 6.5.1.0
140049	**Symptom:** An AP took longer time to boot. This issue is resolved by moving the Diffie Hellman Group 14 (DH14) operation from software to hardware crypto engine. **Scenario:** This issue occurred when CPsec was enabled in a switch. This issue was observed in switches running AOS-W 6.4.3.3-FIPS.	IPsec	All platforms	AOS-W 6.4.3.3-FIPS	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140171 146291	**Symptom:** The switch set the path cost of a mesh portal AP to 3 even when the AP was connected to a 1 Gbps port. The fix ensures that the path cost is 0 when an AP connects to a 1 Gbps port. **Scenario:** This issue was observed in OAW-AP200 Series, OAW-AP207, and OAW-AP210 Series access points running AOS-W 6.4.4.8 or later versions.	Mesh	OAW-AP200 Series, OAW-AP207, OAW-AP210 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.0.0
140206	**Symptom:** In the switch WebUI, **ERROR: Cannot delete the NTP Server** was displayed while configuring the clock using wizard. The fix ensures that the WebUI interprets the CLI configuration correctly. **Scenario:** This issue was observed when NTP server was not configured in the switch. Although the output for the **show ntp servers** brief command was **No Upstream NTP servers configured**, the WebUI failed to interpret the CLI configuration correctly. This issue was observed in switches running AOS-W 6.4.3.4 or later versions.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.1.0
140327 144285 144288 144438 147584	**Symptom:** Memory usage of the **authentication** process in a switch increased gradually. The fix ensures that the memory is freed and used optimally. **Scenario:** This issue occurred because of a memory leak. This issue was observed in switches running AOS-W 6.4.3.3.	Base OS Security	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.1.0
140556	**Symptom:** Logging levels configured for Activate process did not persist after a switch reload, although the appropriate logging level configuration was saved. The fix ensures that the logging levels configured for the Activate process persist even after a reload. **Scenario:** This issue occurred because the Activate did not initialize the logging levels after a reload. This issue was not limited to any specific switch model or AOS-W version.	Activate/OV3600	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.1.0
140805	**Symptom:** Configuring multiple DHCP options in the DHCP pool using the navigation path **Configuration > Branch > Smart config > Routing > DHCP options** in the switch WebUI failed. This issue is resolved by using using the |symbol to seperate the multiple options of DHCP pool. **Scenario:** Thsis issue was observed when DHCP options were separated by a comma. This issue was observed in switches running AOS-W 6.4.3.6.	WebUI	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141073 144233 144932	**Symptom:** The TACACS accounting configuration did not synchronize to local, branch, and standby switches from the master switch. This issue is fixed by correcting the **running-config** command order for AAA TACACS-accounting and ensuring that the TACACS-accounting configuration synchronizes to local, branch, and standby switches. **Scenario:** This issue occurred because of an error in the **running-config** command order. This issue was observed in switches running AOS-W 6.4.4.8.	Base OS Security	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.1.0
141200 142436	**Symptom:** The **iapmgr** process crashed and remained in the **initializing** state in the switch. This issue is resolved by ensuring that the branch ID values do not get corrupted. **Scenario:** This issue was observed in APs functioning as IAP-VPN running AOS-W 6.4.4.x or later versions.	Remote AP	OAW-RAP3WN and OAW-RAP3WNP access points	AOS-W 6.4.4.6	AOS-W 6.5.1.0
141388	**Symptom:** An ethernet port of an OAW-AP330 Series access point failed to form an LACP group. If the link speed is different, executing the **show ap debug lacp** command displays the following message: **NOTE: LACP is disabled on one of the ports due to link speed incompatibility** **Scenario:** The ethernet port of an AP was not added to a link aggregation group if the link speed was different. For example, when an AP's 2.5 Gbps and 1 Gbps ports are connected to a 2.5 Gbps link aggregation ports of a switch, the 1 Gbps port is not added to the link aggregation group. This is due to a link speed incompatibility. LACP works when the link speed is same. This issue was observed in OAW-AP330 Series access points running AOS-W 6.5.x.	AP-Wireless	OAW-AP330 Series access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0
141429 148041 148364 148551 149212	**Symptom:** Access points crashed and rebooted. The log file for the event listed the reason as **Reboot caused by out of memory**. The fix ensures that the issue with the memory is resolved. **Scenario:** This issue was observed in OAW-AP275 access points running AOS-W 6.5.0.0.	AP-Platform	OAW-AP275 access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141693 143220 144785	**Symptom:** A RAP with 340U MODEM for cellular uplink crashed continuously. This issue is resolved by: • Applying newer firmware without LINUX patch on OAW-AP205H access points. • Applying LINUX patch and adding a delay after mode switch to allow population of new device ID on RAP-155 remote access points. **Scenario:** This issue was observed when OAW-AP205H access points and OAW-RAP155 remote access points running AOS-W 6.5.0.0 used 340U MODEM for cellular uplink.	Remote AP	OAW-AP205H access points and OAW-RAP155 access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0
141902	**Symptom:** The **mDNS** process in a local switch crashed unexpectedly. This issue is resolved by changing the output format of the **show airgroup cppm-server radius statistics** and **show airgroup cppm-server rfc3576** statistics commands. **Scenario:** This issue occurred only when the network had more than seven RADIUS servers and the **show airgroup cppm-server radius statistics** or **show airgroup cppm-server rfc3576 statistics** command was executed. These commands showed different RADIUS/RFC3576 server statistics and when the number of servers was more than seven, the number of columns increased and corrupted the memory. This issue was observed in switches running AOS-W 6.4.4.5.	AirGroup	All platforms	AOS-W 6.4.4.5	AOS-W 6.5.1.0
142106	**Symptom:** A switch crashed due to low memory in the **Authentication** process.This issue is resolved by blocking was facing by blocking certain scenarios that leaked memory. **Scenario:** This issue was observed when a packet was sent to port 8082 of the switch. This issue was observed in switches running AOS-W 6.4.2.12 or later versions.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.1.0
142157	**Symptom:** The 5 GHz radio of an AP running in spectrum mode stopped responding. The fix ensures that the 5 GHz radio of an AP does not hang in spectrum monitor mode. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 6.5.0.0.	Spectrum	OAW-AP315 access points	AOS-W 6.5.0.0	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142197	**Symptom:** A client faced connectivity issues when an AP switched channels randomly. This issue is resolved by deleting a timer before it is started in AP mode only. **Scenario:** This issue occurred under the following circumstances: Multiple OAW-AP225 access points did not have a wireless association for a long duration Excessive channel switching occurred because of RADAR detect trigger 5 GHz radio did not accept associations and transmission of frames was stalled until the AP was rebooted This issue was observed in OAW-AP225 access points running AOS-W 6.4.2.14.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.2.14	AOS-W 6.5.1.0
142257	**Symptom:** The **wlanAPName** trap failed to lists all the APs irrespective of the status. With this fix, the **wlanAPName** trap lists all the APs. **Scenario:** This issue was seen when an SNMP walk action was performed on the **wlanAPName** trap. This issue was observed in switches running AOS-W 6.4.3.5.	SNMP	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.1.0
142310	**Symptom:** The status of the IAP table in a switch showed DOWN for some IAPs even though IPsec and client traffic were running. This issue is resolved by deleting the old session if a switch has an existing session for an allocated inner IP address. **Scenario:** This issue occurred when the elected master of an IAP cluster went offline and a new IAP was elected as the master. The switch had two security associations with same inner IP address but different outer IP addresses. This issue was observed in switches running AOS-W 6.4.4.4.	Remote AP	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.1.0
142330 142786 142870	**Symptom:** The OV3600 WebUI showed **802.11ag** as the connection mode for some clients, while the switch WebUI showed **802.11g** as the connection mode for the same clients. This issue is resolved by removing the second mapping of the connection mode to the SNMP MIB value if the connection mode is already mapped in the authentication process. **Scenario:** The issue occurred when the connection mode was mapped twice, once each by the **authentication** process and **SNMP** process resulting in a wrong value. This issue was observed in switches running AOS-W 6.4.4.5.	SNMP	All platforms	AOS-W 6.4.4.5	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142376 142378	**Symptom:** The **datapath** process in a switch crashed and the switch rebooted unexpectedly. The log file for the event listed the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the switch does not reboot due to a datapath timeout. **Scenario:** This issue occurred under the following circumstances: ● When the ARP entry for an IP address aged out or forcefully deleted while traffic was running. ● When jumbo processing was enabled and the switch received a management multi-buffer IP frame. This issue was observed in switches running AOS-W 6.4.4.5.	Switch-Datapath	All platforms	AOS-W 6.4.4.5	AOS-W 6.5.1.0
142395	**Symptom:** The output of the **show boot history** command displayed incorrect user information in the **Reboot Cause** message. However, the correct information was logged in the **Controller Reboot initiated** message before the reload. The fix ensures that the **Reboot Cause** message displays the appropriate information. **Scenario:** This issue occurred because the switch incorrectly used the current user information who logged in and executed the **show boot history** command for the **Reboot Cause** message. This issue was not limited to any specific switch model or AOS-W version.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
142397	**Symptom:** IPv4 syslog messages were interpreted incorrectly due to invalid timestamp format. The fix ensures that the timestamp format is according to the standards. **Scenario:** This issue occurred because the timestamp in the syslog message for IPv4 address included the year at the end, which was not according to the standards. This issue was not limited to any specific switch model or release version.	Logging	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
142449	**Symptom:** The IPv6 static route settings disappeared after the switch reloaded. This issue is resolved by adding a check for interface number match and removing the check in which IPv6 address of the destination was checked against next hop address for equality. **Scenario:** This issue was observed because IPv6 route with link local as the next hop was not added to the kernel after shut and no shut of a VLAN interface. This issue was observed in switches running AOS-W 6.4.4.7 or later versions.	IPv6	All platforms	AOS-W 6.4.4.7	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142514	**Symptom:** The client was unable to set IPv6 unique local address (ULA) as next-hop in static route. This issue is resolved by allowing ULA as the nexthop in static route. **Scenario:** This issue was observed when the kernel did not allow the addition of IPv6 ULA as nexthop in static route. This issue was observed in OAW-4005 switches running AOS-W 6.4.4.6.	IPv6	OAW-4005 switches	AOS-W 6.4.4.6	AOS-W 6.5.1.0
142617	**Symptom:** An AP continued to reboot with the reboot reason **Rebooting after provisioning**. The fix ensures that the AP does not reboot on provisioning the AP with the **master clear** option. **Scenario:** This issue was observed when an AP was provisioned with the **master clear** option and applied to the AP group. This resulted in the AP to reboot in a loop. This issue was observed in APs running AOS-W 6.4.4.6 or later versions.	AP-Platform	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
142678	**Symptom:** Adding an NTP server to the switch caused all the Instant AP VPN /RAP to reconnect without notification. Many Instant AP VPNs could not recover as well. This issue is resolved by displaying a warning message to reboot the switch when NTP servers are added. **Scenario:** This issue occurred when the NTP server tried to correct the time difference in the switch. This issue was not limited to any specific switch model or release version.	IPsec	All platforms	AOS-W 6.4.2.13	AOS-W 6.5.1.0
142682 144337 142682	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot Reason: Reboot caused by kernel panic**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.8.	AP-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.1.0
142722	**Symptom:** switch rebooted continuously and the log files listed the reason for the reboot as **Nanny rebooted machine - fpapps process died**. The fix ensures that the **fpapps** process does not crash. **Scenario:** This issue occurred due to the cellular profile configuration options. This issue was observed in switches running AOS-W 6.5.	Switch-Platform	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142856	**Symptom:** The bandwidth contract was not updated after a role change. This issue is resolved by updating the bandwidth contract when an L2 role is updated. **Scenario:** This issue occurred when the L2 role was changed for a user but the bandwidth contract was not updated if the user did not have an L3 role configured. This issue was observed in switches running AOS-W 6.4.3.7.	Base OS Security	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
142975	**Symptom:**An AP103H access point suddenly stopped forwarding traffic until it was rebooted. The fix ensures that the AP continues to forward traffic. **Scenario:** This issue occurred when a tunnel mode Virtual AP and a bridge mode Virtual AP or wired AP were both configured on a single AP. This issue was not limited to any specific AP model or AOS-W version.	AP-Datapath	All AP platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
143024	**Symptom:** Two 6000 switches in two different clusters crashed. This issue is resolved by ensuring that the memory allocated is freed up while processing 802.11r-related roaming. **Scenario:** This issue occurred when dot11r was enabled in the SSID profile and when the clients performed 802.11r fast BSS transition while roaming. This resulted in memory leakage by the **STM process** of the switch while processing 802.11r-related roaming. This issue was not limited to any specific switch model or AOS-W version.	Station Management	All platforms	AOS-W 6.3.1.x	AOS-W 6.5.1.0
143119	**Symptom:** The browser session took a long to time to terminate when it accessed the switch on port 8082. The fix ensures that any session originating with port 8082 is ignored. **Scenario:** This issue occurred when a http/https session was created with switch ip or any other reachable ip on port 8082, which resulted in a loop due to idp logic on the switch. This issue was observed in OAW-4550 switches running AOS-W 6.4.3.4.	Web Server	OAW-4550 switches	AOS-W 6.4.3.4	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143181	**Symptom:** An OAW-4x50 Series switch continuously contacted the Activate server. This issue is resolved by adding the **acitvate periodic-sync {enable|disable}** parameter in the CLI to control the communication with the Activate server. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.x or later versions.	BOC	OAW-4x50 Series switches	AOS-W 6.4.4.5	AOS-W 6.5.1.0
143185	**Symptom:** A Virtual Intranet Access (VIA) client failed to connect to a switch. This issue is resolved by clearing the IP addresses from the Layer 2 Tunneling Protocol (L2TP) used pool when a Security Association (SA) is deleted for a VIA client. **Scenario:** This issue occurred when a VIA client did not get an IP address from the L2TP pool because the L2TP pool was exhausted. This issue was observed in switches running AOS-W 6.4.3.7.	L2TP	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
143278	**Symptom:** The search feature in the **Dashboard > Clients** page of the WebUI did not work for an IP address. This issue is resolved by adding the IP address of the access points in the dashboard search. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.6.	WebUI	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
143342	**Symptom:** On configuring a custom IPv6 link-local address, the switch failed to display the configuration in the running configuration of the switch. This issue is resolved by setting a flag for the custom IPv6 link-local address. **Scenario:** This issue was observed when the neighbor discovery and router advertisement settings were enabled. This issue was observed in switches running AOS-W 6.4.4.6.	IPv6	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
143444	**Symptom:** A switch dropped some packets. This issue is resolved by adding a mask to take only the lower 12 bits for the VLAN ID. **Scenario:** This issue occurred because a switch dropped all VLAN priority tagged packets. This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
143684	**Symptom:** The result of AP search in the WebUI showed more access points than the number of results per page. This issue is resolved by showing the correct result of AP search in the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.8.	WebUI	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143744	**Symptom:** The **Acct-Input-Octets** and **Acct-Output-Octets** always showed 0 in RADIUS accounting messages. This issue is resolved by converting the byte order before writing it into the RADIUS accounting message. **Scenario:** This issue occurred for users in split-tunnel forwarding mode. This issue was observed in OAW-AP205 access points running AOS-W 6.4.3.6.	AP-Platform	OAW-AP205 access points	AOS-W 6.4.3.6	AOS-W 6.5.1.0
143827	**Symptom:** An OAW-4030 master switch rebooted due to a datapath process crash. The log file for the event listed the reason as **Datapath timeout (Intent:cause:register 56:86:50:60)**. This issue is resolved by dropping the packets that contain invalid tunnel entries. **Scenario:** This issue occurred when invalid tunnel entries were processed by the switch. This issue was not limited to any specific switch model or AOS-W version.	Switch-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.1.0
143931	**Symptom:** On a VRRP standby switch, the custom captive portal background image is not displayed in the preview page. When the VRRP standby switch becomes the master switch, captive portal users see a black page instead of a custom background image. This issue is resolved by: ● Disabling **database synchronize captive-portal-custom**. ● Creating a new captive portal profile and uploading the background image and custom captive portal page on both master and standby switches. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.4 in a master-standby topology.	Database	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.1.0
143967	**Symptom:** An administrator failed to configure SHA1-96 hash within IKEv2 ISAKMP policy in a switch running FIPS build. This issue is resolved by allowing SHA1-96 hash configuration for FIPS build. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.x-FIPS or AOS-W 6.4.x.x-FIPS.	IPsec	All platforms	AOS-W 6.3.1.5-FIPS	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144082	**Symptom:** Few MIB OIDs did not work after upgrading to AOS-W 6.4.x. This issue is resolved by adding counters to ensure that all the association/reassociation requests were counted correctly. **Scenario:** This issue was observed as only the successful associations/reassociations were counted instead of the total number of them by the STM. This issue was observed in OAW-4750 switches running AOS-W 6.4.4.5.	SNMP	OAW-4750 switch	AOS-W 6.4.4.5	AOS-W 6.5.1.0
144229	**Symptom:** A user cannot configure the CPPM credentials under **RADIUS Server** in the **Servers** tab of the **Configuration > Security > Authentication > Servers** page of the WebUI. The fix ensures that the CPPM credential configuration is successful from the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x and AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.3.9	AOS-W 6.5.1.0
144262 145804 145814 149047	**Symptom:** Some client devices (vendor-specific) were unable to get their respective DHCP IP address on WPA2-PSK-AES or 802.1x-EAP SSID. This issue was not seen in devices with Open or WPA2-PSK-TKIP SSID. This fix ensures that clients are able to get their respective DHCP IP address. **Scenario:** The issue was triggered when reprovisioning an AP from a group with HT-enabled rf-profile to that with a HT-disabled rf-profile.	AP-Platform	OAW-AP200 Series, OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP228, and OAW-AP270 Series access points	AOS-W 6.4.3.9	AOS-W 6.5.1.0
144700	**Symptom:** The **datapath** process in a switch crashed and the switch rebooted unexpectedly. The log file for the event listed the reason as **Datapath timeout**. This issue is resolved by dropping the packets that come over the mobility tunnel from Home Agent (HA) to Foreign Agent (FA) if they cause a bridge miss. **Scenario:** This issue occurred when packets coming over the mobility tunnel from HA to FA caused a bridge miss. This issue was observed in switches running AOS-W 6.4.3.6.	Switch-Datapath	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144703	**Symptom:** The LLDP packets from a client were dropped. The fix ensures that the LLDP packets are not dropped and are correctly delivered to Linux stack. **Scenario:** This issue occurred when the **spanning tree** option was enabled on the Ethernet (POE enabled) port of a RAP. This issue was observed in remote access points running AOS-W 6.4.3.9.	Remote AP	All platforms	AOS-W 6.4.3.9	AOS-W 6.5.1.0
144768 145436	**Symptom:** OAW-AP135 access points rebooted when a Hotspot 2 client sent a request for a parameter defined in the STM process. This issue is resolved by making changes to the logic used to parse the ANQP request. **Scenario:** This issue occurred due to incorrect array size checking before deferring array. This issue was observed in OAW-AP135 access points running AOS-W 6.4.2.17.	Hotspot	OAW-AP135 access points	AOS-W 6.4.2.17	AOS-W 6.5.1.0
144843	**Symptom:** Policy Based Routing (PBR) did not work in a switch when the nexthop-list exceeded 24 characters. This issue is resolved by increasing the nexthop-list policy name size to 128 characters. **Scenario:** This issue occurred when the nexthop-list policy name exceeded 24 characters. This issue was observed in switches running AOS-W 6.4.4.6.	Policy Based Routing	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
145314	**Symptom:** An OAW-AP325 access point crashed. The log file for the event stated the reason as **Kernel panic – not syncing: Rebooting the AP because of FW ASSERT**. This issue is fixed by rejecting the client association request with a higher NSS value. **Scenario:** This issue occurred when the NSS value in the client association request was higher than the supported NSS value. This issue was observed in OAW-AP300 Series access points running AOS-W 6.4.x version.	AP-Platform	OAW-AP300 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0
145373	**Symptom:** High noise floor was observed due to increase in traffic load on OAW-AP225. The fix ensures that the vendor driver is upgraded to resolve the issue with the noise floor. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.4.4.8.	AP Platform	OAW-AP225 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145458	**Symptom:** No data was presented when the client sorted the table by any column other than default. The issue is resolved by removing an invalid internal filter added automatically when sorting by any column other than default. **Scenario:** The system displayed a **no matches found** message, when the user navigated to **Dashboard > Clients**, selected a client and clicked on **Traffic > Application > Bytes** column. This issue was observed in OAW-4010 switches running AOS-W 6.5.0.0.	Web UI	OAW-4010 switches	AOS-W 6.5.0.0	AOS-W 6.5.1.0
145486 146896 148292	**Symptom:** The configuration on the master switch was not synchronized with the local switch. The fix ensures that the synchronization issue is resolved. **Scenario:** Although centralized licensing was enabled and synchronized and licenses were available, access points displayed the **IL** flag. This issue was observed in OAW-4750 switches running AOS-W 6.4.3.7.	Master-Local	OAW-4750switches	AOS-W 6.4.3.7	AOS-W 6.5.1.0
145634	**Symptom:** An AP crashed unexpectedly. The log file of the event listed the reason as kernel panic. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP215 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0
145658	**Symptom:** A switch crashed when the size of /tmp/.fpcli_cfg_diff and /tmp/.fpcli_cfg_diff_enc temporary files increased. The issue is resolved by adding a size limit of 1MB for these files and if the limit crosses 1 MB, the **show configuration diff** command will display a warning. **Scenario:** This issue occurred when the ip routes were added and removed continuously using a script and the **#write mem** command was not performed. This issue was observed in switches running AOS-W 6.3.1.18.	Switch-Platform	All platforms	AOS-W 6.3.1.18	AOS-W 6.5.1.0
145755	**Symptom:** A wired port initiated UDP 4500 went outside a branch office switch although an IP route existed. This issue is resolved by allowing inner tunnel when the destination of the inner tunnel is not the master switch. **Scenario:** This issue occurred because an IPsec tunnel inside a master-local IPsec tunnel was not supported. This issue was observed in branch office switches running AOS-W 6.4.4.9.	BOC	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145803	**Symptom:** The switch was unable to generate **wlsxNConnectionBackfromLocal** trap although the trap is enabled. The fix ensures that the switch is able to generate the SNMP trap. **Scenario:** This issue occurred when the local switch was reloaded and the master switch did not generate the wlsxNConnectionBackfromLocal trap. This issue was observed in switches running AOS-W 6.4.4.6.	SNMP	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.1.0
146000	**Symptom:** The current Software Development Kit (SDK) did not support long URL classification as part of Web Content Classification (WebCC). This issue is resolved by updating the SDK to the latest build. **Scenario:** This issue was observed in switches running AOS-W 6.4.x and AOS-W 6.5.x.	WebCC	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.1.0
146209	**Symptom:** An AP requested more PoE power than the maximum power consumption. This issue is resolved by reducing the requested PoE power from 25.5 W to 23 W. **Scenario:** This issue was observed in OAW-AP228 access points running AOS-W 6.4.4.8	AP-Platform	OAW-AP228 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0
146358	**Symptom:** An LACP/VRRP link toggled frequently on the master switch. This issue is resolved by ensuring that the IPv4/IPv6 VRRP packets are received and processed as expected. **Scenario:** This issue was observed when the switch was upgraded to AOS-W 6.4.3.7. In addition, this issue was seen on the master switch in a master-local topology. This issue was seen in switches running AOS-W 6.4.3.0 and AOS-W 6.4.3.7.	Switch-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.0
146455	**Symptom:** APs randomly failed to scan the nearby BLE devices. This issue is resolved by correcting the erroneous check for detecting any AP stuck in bank A, and by adding periodical checks to make sure the BLE device operates in the correct bank (bank B). **Scenario:** This issue was seen in OAW-AP200 Series and OAW-AP300 Series access points running AOS-W 6.4.3.x and AOS-W 6.4.3.7.	BLE	OAW-AP200 Series and OAW-AP300 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146564	**Symptom:** The LLDP negotiation was not correct in an AP. This issue is resolved by adding a delay while shutting down an Ethernet port of an AP if input power is detected. If the LLDP message suggests that power is good, the AP can use both Ethernet ports when input power is detected. **Scenario:** This issue occurred when the eth1 port of an OAW-AP325 access point was connected before its eth0 port was connected to a POE+ switch. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0
146653	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **kernel panic at 0x009C07BC**. The fix ensures that an AP works as expected. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.0
146836	**Symptom:** In the WebUI, while trying to apply the reordered policies for a new user role, the following error was displayed: **Position 1 and 2 are reserved for Global and Role default session**. This issue is resolved by incorporating code changes that handle the reordering of policies properly when creating a new user role. **NOTE:** This fix is applicable only to the **Choose from Configured Policies** option available in the **Firewall Policies** tab. This fix is NOT applicable for the following options: **Create New Policy From Existing Policy** and **Create New Policy**. **Scenario:** This issue occurred when the **Apply** button was clicked after reordering the policies for a new role. This issue was not limited to any specific platform or AOS-W release version.	UI-Configuration	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.1.0
146911	**Symptom:** Clients using VIA were unable to connect to the switch after the **ISAKMPD** process crashed. This issue is resolved by changing the IKE context storing and handling. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.14.	IPsec	All platforms	AOS-W 6.3.1.14	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146945	**Symptom:** EAPOL packets were marked according to WMM-eap-ac config in the SSID profile, but an AP ignored the dscp-dot1p-priority-mapping configuration. Hence, the dot1p marking was default according to the DSCP value. This issue is resolved by clearing the old 802.1P value before setting a new value for a particular DSCP value. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 6.5.1.0.	AP-Platform	OAW-AP200 Series access points	AOS-W 6.5.1.0	AOS-W 6.5.1.0
147008	**Symptom:** Datapath timeout occurred in an OAW-4750 switch and the switch rebooted with the reboot cause stating **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:60)**. This issue is resolved by updating the new SDK that has the fix for handling large URLs. **Scenario:** This issue occurred due to the use of large URLs. This issue was observed in switches running AOS-W 6.4.3.9.	Switch-Datapath	All platforms	AOS-W 6.4.3.9	AOS-W 6.5.1.0
147157	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **AP-105 Reboot caused by kernel page fault at virtual address 00000ad4, epc == c08a2c88, ra == c088fc18**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP105 access points running AOS-W 6.4.3.3.	AP-Wireless	OAW-AP105 access points	AOS-W 6.4.3.3	AOS-W 6.5.1.0
147195	**Symptom:** The value of **NAS-Port-Type** RADIUS attribute was set to **19 (Wireless-User-Type)** when the Remote Access Point (RAP) was authenticated with the external server. This issue is resolved by setting the value of the **NAS-Port-Type** to **15 (Wired-User-Type)**. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.16.	RADIUS	All platforms	AOS-W 6.3.1.16	AOS-W 6.5.1.0
147382 148123	**Symptom:** A Remote AP with 313U USB MODEM did not boot on cellular uplink. The fix ensures that the remote AP boots using 313U MODEM as uplink. **Scenario:** This issue was observed in OAW-RAP3WN remote access points using 313U USB MODEM for uplink and running AOS-W 6.4.4.9.	Remote AP	OAW-RAP3WN	AOS-W 6.4.4.9	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
147462	**Symptom:** The IP address for some of the bridge mode users was not populated in the **Clients** page in OV3600. The fix ensures that the IP address for the bridge mode users is populated. **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 6.4.3.5.	Base OS Security	OAW-4550 switches	AOS-W 6.4.3.5	AOS-W 6.5.1.0
147638	**Symptom:** A switch failed to respond and rebooted. This issue is resolved by altering the STM process and adding more robustness when handling incoming **Hello** request. **Scenario:** This issue was not limited to a specific switch model or AOS-W version.	AP-Platform	All platforms	AOS-W 6.5.1.0	AOS-W 6.5.1.0
147667	**Symptom:** When the client attempted to change the cellular network preference from 3G to 4G or vice-versa, the AP got an IP address after a long duration and multiple attempts. The fix ensures that there is a seamless switch to the new network by resetting the modem in the software when there is a mode switch. **Scenario:** This issue was observed when the mode switch was not seamless while switching to another network. This issue was observed in switches running AOS-W 6.3.1.19.	Remote AP	All platforms	AOS-W 6.3.1.19	AOS-W 6.5.1.0

Table 3: *Resolved Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
147749 148987	**Symptom:** Wireless clients observed performance and connectivity issue on the wireless network. The fix ensures that the clients stay connected without any performance degradation. **Scenario:** The **STM** (Station Management) process stopped responding and crashed. The log file for the event listed the reason as **segmentation fault**. This issue occurred when the switch received corrupted packets. This issue was observed in switches running AOS-W 6.4.3.x or later versions.	Station Management	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.1.0
147959 148668	**Symptom:** The configuration on the local switch was truncated and the ap-groups were lost after master-local synchronization. The fix ensures that the issue with the truncation of configuration on the local switch is resolved. **Scenario:** This issue was observed in OAW-4650 switches running AOS-W 6.4.3.10.	Master-Local	OAW-4650 switches	AOS-W 6.4.3.10	AOS-W 6.5.1.0
148630	**Symptom:** DHCP Diff timestamps were sent as part of DHCP AMON messages. This issue is resolved by optimizing the calculation of the DHCP Diff stamp to improve the precision of DHCP Diff values that are sent as part of the DHCP AMON message. **Scenario:** This issue was not limited to any specific switch model or AOS-W version. The issue was observed in a generic DHCP/AMON setup.	Clarity-Live	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.1.0

Chapter 5
Known Issues

This section describes the known and outstanding issues identified in AOS-W 6.5.1.0.

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
96739	**Symptom:** : The **Clients** page in the switch WebUI does not display user-related information such as **User Name**, **Client IP**, **User Role**, and **Device Type**. **Scenario:** This issue is observed in the **Monitoring > Controller > Clients** page of the WebUI after upgrading the switch from the AOS-W 6.1.3.10 to AOS-W version. **Workaround:** None.	AMON	All platforms	AOS-W 6.3.1.2
109921	**Symptom:** When a Pre-Shared Key (PSK) in the SSID profile is configured it cannot contain single quotes, double quotes, and blank spaces in the same passphrase. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.3.1.10. **Workaround:** None.	AP-Platform	OAW-4550 switches	AOS-W 6.3.1.10
115215	**Symptom:** The Co-Channel Interference (CCI) test causes false non-wifi-interference in the output of the **show ap radio-summary** command. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.5. **Workaround:** None.	ARM	All platforms	AOS-W 6.4.2.5

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
119350	**Symptom:** The WLAN count for APs in the **Dashboard > Access Points** page is incorrect when a Virtual AP is configured using **AP Name** specific configuration. **Scenario:** An increment in WLAN count is observed when an AP for which the Virtual AP is configured using **AP Name** specific configuration is rebooted. This issue is observed in switches running AOS-W 6.4 and prior versions. **Workaround:** None.	Monitoring	All platforms	AOS-W 6.4.2.8
121019	**Symptom:** A few wireless clients are marked as internal in the user-table and assume ap-role. **Scenario:** This issue occurs when some wireless clients are assigned with the commonly used nonpublic IP addresses such as 192.168.1.*. These IP addresses clash with the AP's IP address. This issue is observed in switches running AOS-W 6.4.2.5 in a master-standby topology. **Workaround:** Do not assign commonly used non-public IP-addresses to APs.	Base OS Security	All platforms	AOS-W 6.4.2.5
126244 133950 136632 136957	**Symptom:** An AP entry disappears from the local switch database but displays as **UP** in the master switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.5 in master-local topology. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.5
127094 138590 144730	**Symptom:** The **Dashboard > Access Points > Radios** page of the WebUI displays some of the AP names as **unknown**. **Scenario:** This issue occurs during a HA failover when the AP switches from the master switch to a standby switch. This issue was not limited to any specific AP model or AOS-W version. **Workaround:** None.	AP-Platform	All AP platforms	AOS-W 6.4.2.12

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
127941	**Symptom:** OAW-AP225 access point crashed unexpectedly. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.3.2. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.3.2
128448	**Symptom:** A switch crashes and reboots unexpectedly. **Scenario:** After upgrading the switch from AOS-W 6.3.1.2 to AOS-W 6.4.4.1, the switch crashes while running some SNMPv3 queries if configured with VRRP. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.1. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.4.1
129149	**Symptom:** The switch displays a non-configured WLAN SSID called **wired** in the **Dashboard > AppRF > WLAN > Details** section of the WebUI. **Scenario:** This issue occurs even when no WLAN SSID with the 'wired' name is configured in the switch. This issue is observed in switches running AOS-W 6.4.2.8 or AOS-W 6.4.3.7. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 6.4.2.8
129565	**Symptom:** Video calls pixelates on Wired Phones(Cisco 9971)only when connecting to the wired port of Remote-Mesh-Portal. **Scenario:** This issue occurs when a video call is initiated from a wired Cisco 9971 phone that connects to the Ethernet port of an OAW-RAP155 (Mesh-Point) to another wired Cisco 9971 phone that connects to the Ethernet port of another OAW-RAP155 (Remote-Mesh-Portal), the video pixelates only on the Mesh-Portal end. This issue is observed in OAW-RAP155 running AOS-W 6.3.1.15 or later versions.. **Workaround:** None.	Mesh	OAW-RAP155	AOS-W 6.3.1.15
130189	**Symptom:** When the Enet-0/1 cable is switched to a different port on the switch or stack, access points do not come up. **Scenario:** This issue is observed in OAW-AP324 and OAW-AP325 access points running AOS-W 6.4.4.2. **Workaround:** None.	AP-Platform	OAW-AP324 and OAW-AP325 access points	AOS-W 6.4.4.2

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
133036	**Symptom:** A ??? switch encounters kernel panic. **Scenario:** This issue occurs when the USB reclassification happens many times, when a cellular modem—that is, modem models E3276 and E3372 (one that is not supported in AOS-W 6.5.0.0)— is connected as uplink to the switch in addition to the wired uplink. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Either plug out and plug in the modem or reboot the switch.	Switch-Platform	All platforms	AOS-W 6.5.0.0
134464 145568	**Symptom:** The **spectrum-mode** configuration in the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** is not synchronized between the master and backup switch. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.4.4.8. **Workaround:** Add rfp license on the standby switch.	Licensing	OAW-4750 switches	AOS-W 6.4.4.8
135926	**Symptom:** After an Instant AP (IAP) or the VPN tunnel loses connectivity and returns to service, the nodes connected to VPN-NG centralized L2 VLANS behind IAPs becomes unreachable from behind the switch through the VPN tunnels. The switch shows L3 ARP entry for the node, but does not show L2 entry. **Scenario:** This issue is observed when an Instant AP is connected to a centralized switch through VPN-NG IPSEC tunnels configured for centralized L2 operations with Broadcast Multicast (BCMC) optimization configured on the VLAN. When the VPN tunnel is down, the switch deletes the learned L2 entries, but incorrectly keeps the L3 ARP entries. Once the VPN tunnel re-establishes, since the ARP entry exists, subsequent ARP frames are not flooded to the IAP and are not answered by the client allowing L2 re-learning. **Workaround:** Disable BCMC optimization on the affected VLAN by executing the following commands: **(host) (config) #interface vlan <VLAN>** **(host) (config-subif)#no bcmc-optimization**	RAP-NG	All platforms	AOS-W 6.4.2.14

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
136419	**Symptom:** The centralized licensing feature does not support a topology where a local license client switch is associated to a licensing master connected to both a master license client switch and a redundant licensing server. **Scenario**: This deployment model is not supported in AOS-W 6.5.1, as the master switch in this topology is unable to configure the license server VRRP IP address for the local switch. **Workaround**: None.	Licensing	All platforms	AOS-W 6.5.0.0
138009	**Symptom:** An OAW-4650 switch (local) reboots because of datapath timeout. **Scenario:** This issue occurs after the local switch—supporting more than 1000 RAPs and 3000 wireless clients—is upgraded to AOS-W 6.4.2.15. This issue is observed in OAW-4650 switches running AOS-W 6.4.2.15 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4650switches	AOS-W 6.4.2.15
138224	**Symptom:** A switch does not generate the syslog message 124821 when a remote AP has loop on Ethernet ports. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.16. **Workaround:** None.	Remote Access Points	All platforms	AOS-W 6.3.1.16
138808	**Symptom:** An error in AP wireless containment is observed. **Scenario:** This issue is observed when the access point functional in the AM mode is unable to send containment related frames. This issue is observed in OAW-AP205 access points running AOS-W 6.4.3.6. **Workaround:** None.	Air Management - IDS	OAW-AP205 access points	AOS-W 6.4.3.6
139377	**Symptom:** Datapath bandwidth contract is not being applied to random users. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.3.2. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.2

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
139962	**Symptom:** Customer notices that stale entries are present in association tables. **Scenario:** The stale entries are present in both the switch and the AP association tables but not in the AP driver's client table. This issue is observed in OAW-AP90 Series and OAW-AP100 Series access points running AOS-W 6.4.2.x. **Workaround:** An AP reboot will clear the stale entries.	Station Management	OAW-AP90 Series and OAW-AP100 Series access points	AOS-W 6.4.2.12
140721	**Symptom:** An OAW-AP103H access point reboots randomly without providing any reboot information. **Scenario:** This issue is observed in OAW-AP103H access points running AOS-W 6.4.4.4. **Workaround:** None.	AP-Platform	OAW-AP103H access points	AOS-W 6.4.4.4
141285	**Symptom:** The ports in a switch move to **DOWN** state unexpectedly. **Scenario:** This issue is observed in OAW-4x50 Series switchesrunning AOS-W 6.5.0.0. **Workaround:** None.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.5.0.0
141455	**Symptom:** The **ARM**, **LLDP**, and **mDNS**processes in a switch crash unexpectedly. The **STM** process in the switch uses more memory than usual. All access points connected to a switch reboot. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.12. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.2.12
141558	**Symptom:** The Captive Portal redirection fails when using HTTP. **Scenario:** This issue occurs because the redirect URL from Captive Portal is appended with a string, **&arubalp**, when using HTTP. This issue is observed in switches running AOS-W 6.4.4.x or later versions. **Workaround:** Bypass the Captive Portal landing page to avoid this issue.	Captive Portal	All platforms	AOS-W 6.5.0.0

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
142101	**Symptom:** The master switch does not list the Motorola RF Scan Gun when the **show user-table** command is executed. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.16. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.3.1.16
142663	**Symptom:** The command-line interface does not prompt for a reboot the first time a license is installed on a switch using centralized licensing. **Scenario:** When you install a license on a switch, you must reboot that device before the license is activated. An issue is observed where the command-line interface fails to display a reminder to prompt the user to reboot the switch. **Workaround:** None.	Licensing	OAW-4x50 Series and OAW-40xx Series switches	AOS-W 6.3.2.0
143101	**Symptom:** Clients fail to connect to an SSID. The log files for the event lists the reason as **Capability requested by STA unsupported by AP**. **Scenario:** This issue is seen in an HA failover when the AP connects back to its original switch. This issue is observed in OAW-AP320 Series access points running AOS-W 6.5.0.0. **Workaround:** None.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.5.0.0
143566	**Symptom:** The error **Module authentication is busy. Please try later.** is displayed when the command, **show reference user-role game-guest** is executed. **Scenario:** This issue is observed in a master local topology with switches running AOS-W 6.4.2.16. **Workaround:** None.	Configuration	All platform	AOS-W 6.4.2.16
143753	**Symptom:** A switch does not show DSCP tagging for ESP packets. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.5. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.5

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
143836	**Symptom:** When an Instant AP is deployed as a Campus AP, it is unable to come up on the switch using the 4G uplink. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.2.12. **Workaround:** None.	AP-Platform	OAW-4650 switches	AOS-W 6.4.2.12
144156 145374 145759	**Symptom:** A multiple process crash is observed on switches due to kernel panic. **Scenario:** This issue is observed when switches are either inaccessible or the user is unable to execute commands on the switches. This issue is observed in OAW-4010 switches running AOS-W 6.4.2.15. **Workaround:** None.	Switch-Platform	OAW-4010 switches	AOS-W 6.4.2.15
144466	**Symptom:** The datapath and Web CC modules on a master switch crashed and the device rebooted. **Scenario:** This issue is observed in OAW-4030 switches running AOS-W 6.4.3.7 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4030 switches	AOS-W 6.4.3.7
144558 141308 146838 147574	**Symptom:** A local switch reports incorrect number of used licenses to the master switch. **Scenario:** This issue is observed when switches are deployed with HA enabled. The AP licenses consumed on a switch can be higher than the overall active licenses present on the switch. This issue is observed in switches running AOS-W 6.4.3.x or later versions. **Workaround:** Restart **STM** process on the switch (issue the **process restart stm** command).	AP-Platform	All platforms	AOS-W 6.4.3.7
144752 146289 146692 146857	**Symptom:** Wired users are incorrectly placed in **default-iap-role** in the switch. The log file for the event lists the reason as **IAP L2 User**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.5 and AOS-W 6.5.x. **Workaround:** None.	Role/VLAN Derivation	All platforms	AOS-W 6.4.4.8

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
145803	**Symptom:** A switch does not generate the **wlsxNConnectionBackfromLocal** trap. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.6
146158	**Symptom:** Access points crashed and rebooted due to kernel panic. The log file for the event lists the reason as **Fatal exception at NIP d98945d4 LR d988a998 CTR: c000c724**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.15. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.2.15
146273	**Symptom:** Users fail to connect to the network after a HA failover. **Scenario:** This issue occurs due to an EAP authentication failure. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.8
147300	**Symptom:** A switch fails to respond and reboots. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.6
147895	**Symptom:** Skype for Business call quality visibility is not available for remote client associated to OAW-AP305 access point in split-tunnel forwarding mode. **Scenario:** UCC score fails to get computed and the **show voice real-time-analysis** command does not display any real-time analysis data for remote clients. This issue is observed in OAW-AP305 access points running AOS-W 6.5.1.0. **Workaround:** None.	UCC	OAW-AP305 access points	AOS-W 6.5.1.0

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
148053	**Symptom:** A local switch reboots unexpectedly. The log file for the event lists the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.4.9
148103	**Symptom:** One-way audio is observed in Vocera communication badges. **Scenario:** This issue is observed under the following circumstances: - The clients performs an L3 roaming. - The roamed client makes a call to a client associated to the switch as a local client. For the roamed client, the switch acts as a foreign agent. This issue is observed in switches running AOS-W 6.4.2.x or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 6.4.2.13
148113	**Symptom:** A client fails to get an IP address when it roams between APs. **Scenario:** This issue is observed under the following circumstances: - L3 mobility is enabled globally. - mobile-IP is disabled on virtual AP. Mobile-IP incorrectly programs the bridge entry even when the client roams across APs terminating on the same switch. This issue is observed in switches running AOS-W 6.4.2.8. **Workaround:** None.	Mobility	All platforms	AOS-W 6.4.2.8
148172	**Symptom:** Unable to create VLANs as Trusted in BOC interface. **Scenario:** This issue is observed in master-branch switch setup. This issues is persistent even after upgrading to AOS-W 6.5.0.0. **Workaround:** None.	WebUI	OAW-4x50 Series switches	

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
148249 148251 148252 148263	**Symptom:** An OAW-4005 switch becomes inaccessible after it is rebooted by unplugging the power multiple times. **Scenario:** This issue occurs when aswitch is hard rebooted multiple times immediately after saving the configuration. This issue is limited to OAW-4005 switch model. **Workaround:** Reset the switch to factory default configuration.	Switch-Platform	OAW-4005 switches	AOS-W 6.4.3.9
148292	**Symptom:** Although centralized licensing is enabled and synchronized and licenses are available, access points displayed the **IL** flag. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7. **Workaround:** None.	Licensing	All platforms	AOS-W 6.4.3.7
148359	**Symptom:** Clients are unable to connect to access points as they are de-authenticated by the AP. The log files for the event lists the reason as **Ageout AP & Ptk Challenge Failed**. **Scenario:** This issue is observed in OAW-AP325 access points running AOS-W 6.4.4.6. **Workaround:** Reboot the AP.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.6
148416	**Symptom:** A crash is observed in the Station Management (STM) module. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.4.3.4. **Workaround:** None.	Station Management	OAW-4550 switches	AOS-W 6.4.3.4
148461	**Symptom:** The switch's Auth Manager logs frequently show the **file user.c function decrement_authserver_outstanding_auths line 10756 error decrement_authserver_outstanding_auths err** error message. **Scenario:** This issue occurs when the increment and decrement in the **outstanding_auths** parameter are out of sync. This issue is observed in OAW-4005 switches running AOS-W 6.4.2.16 in a master-standby topology. **Workaround:** None.	Base OS Security	OAW-4005 switches	AOS-W 6.4.2.16

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
148557	**Symptom:** Clients observed a sudden increase in the number of DHCPv6/Multicast messages from the access points. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9. **Workaround:** None.	AP-Platform	OAW-4650 switches	AOS-W 6.4.4.9
148649	**Symptom:** Clients that connect to OAW-AP105 access points experience less speed. **Scenario:** This issue occurs because the AP's Tx performance is low while its Tx missed acknowledgment rate is high. This issue is observed in OAW-AP105 access points running AOS-W 6.4.4.9. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.9
148674	**Symptom:** The **http** process in a switch is busy. **Scenario:** This issue occurs because of Airwave bootstrapping. This issue is observed in switches running AOS-W 6.4.4.8. **Workaround:** Disable Airwave bootstrapping.	WebUI	All platforms	AOS-W 6.4.4.8
148843	**Symptom:** An internal .IP address (L2TP pool) is getting automatically redistributed when an IAP comes up. **Scenario:** This issue is observed in switches configured with OSPF and when IAP comes up and redistributes OSPF. This issue is observed in OAW-4005 switches running AOS-W 6.4.4.9 and IAP-205 running AOS-W 6.4.2.0-4.1.1.1 **Workaround:** None.	RAP-NG	OAW-4005 switches and IAP-205 access points	AOS-W 6.4.4.9
148885	**Symptom:** When the 802.11g basic rate and tx-rate is set to 12 Mbps, the access point uses only 11 Mbps to send the RTS frame. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.3.6. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.3.6

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
148909	**Symptom:** Local switches in a master-local set up become unresponsive and the user is unable to access the switches through the console. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.4.4.9. **Workaround:** None.	Switch Platform	OAW-4750 switches	AOS-W 6.4.4.9
148962	**Symptom:** An AP crashes and reboots. The reboot cause states that **Reboot caused by kernel panic: Fatal exception in interrupt**. **Scenario:** This issue occurs when there is no client association and the AP is in forward-tunnel mode with multiple VAPs in the network. This issue is observed in OAW-AP205 access points running AOS-W 6.4.3.7. **Workaround:** None.	AP-Wireless	OAW-AP205 access points	AOS-W 6.4.3.7
148991	**Symptom:** Access points are crashing and rebooting. The log file for the event lists the reason as **FW ASSERT**. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 6.5.0.0 in a master-local topology. **Workaround:** None.	AP-Wireless	OAW-AP315 access points	AOS-W 6.5.0.0
148995	**Symptom:** Syslog server displays a lot of error messages. **Scenario:** This issue is observed in an OAW-4750 switch when the user upgrades the switch from AOS-W 6.4.4.8 to AOS-W 6.4.4.9. This issue is caused by the debug info feature that tracks stack usage. **Workaround:** Disable debug info print.	AP-Platform	OAW-4750 switches	AOS-W 6.4.4.9

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
149062	**Symptom:** Whitelist-db entries for control plane security (CPsec) APs are deleted automatically. **Scenario:** This issue occurs due to a reboot of the switch to which the APs are connected. This issue occurs in the following scenarios: - APs are connected to non-Alcatel-Lucent PoE switches, in a set of three in two different switches - Power failure occurs in a switch and all the three APs associated to it also got rebooted, since they are drawing power from the switch. - When the Whitelist-db entries for all the 6 APs get removed from the switch, the APs go to denied state. This issue is observed in OAW-4450 switches in stand-alone master topology running AOS-W 6.4.3.9. **Workaround:** Add the whitelist-db entries for the CPsec APs.	Base OS Security	All platforms	AOS-W 6.4.3.9
149131	**Symptom:** A switch sends only primary port information through AMAP of the LACP link. **Scenario:** This issue occurs when the port-channel interfaces and AMAP are enabled and the packets are sent on the port-channel interfaces rather than individual interfaces. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.10

149142	**Symptom:** Clients fail to renew IP address after roaming away from the native switch.
	Scenario: This issue occurs when **option-82** is enabled on the user VLAN. This issue is not limited to any specific switch model or AOS-W version.
	Workaround: Disable **option-82** on interface using the following commands:
	For L2 VLAN:
	`(host) (config) #no vlan 20 option-82`
	For L3 VLAN:
	`(host) (config) #interface vlan 1.`
	`(host) (config-subif)#no option-82`
		DHCP	All platforms	AOS-W 6.5.0.1

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
149176	**Symptom:** Switches in a master-local topology display profile errors due to which APs fail to come up on the switch. **Scenario:** This issue is observed on OAW-4750 switches running AOS-W 6.4.3.7. **Workaround:** None.	Master-Local	OAW-4750 switches	AOS-W 6.4.3.7
149204	**Symptom:** A switch crashes unexpectedly. The log file lists the reason for the event as **Datapath timeout (Intent:cause:register 56:86:50:2)**. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.2.6
149211	**Symptom:** A **stm** process in a switch crashes unexpectedly. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.8. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.4.8
149367	**Symptom:** Clients using OAW-AP225 access points experience a drop in performance and packet loss. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.3.7. **Workaround:** None.	AP-Wireless	OAW-4650 switches	AOS-W 6.4.3.7

149372	**Symptom:** Clients fail to connect to some APs randomly until the APs are rebooted.
	Scenario: This issue occurs after a channel change is triggered on the APs due to a RADAR detection. This issue is observed on APs running AOS-W 6.4.4.6 or later versions.
	Workaround: Disable channel switch announcement on the AP using the following CLI command:
	`(host) (config) #rf dot11a-radio-profile default`
	`(host) (802.11a radio profile "default") #no csa`
		AP-Wireless	All AP platforms	AOS-W 6.4.4.6

Table 4: *Known Issues in AOS-W 6.5.1.0*

Bug ID	Description	Component	Platform	Reported Version
149550	**Symptom:** Stale entries are seen in the STM client table as compared with the driver. So, the **show ap remote dbug association ap-name** command output has more entries shown as **Associated** than the output of the **show ap debug client-table** command. The output of the **show ap association ap-name** also has many entries. **Scenario:** This issue is seen if APs are up for several weeks. This issue is observed in OAW-AP100 Series and OAW-AP130 Series access points running AOS-W 6.4.4.8 or later versions. **Workaround:** Restart **stm** process on AP (issue **ap process restart ap-name <name> stm**) or restart AP	Station Management	OAW-AP100 Series and OAW-AP130 Series access points	AOS-W 6.4.4.8
149555	**Symptom:** On rebooting the master switch, APs do not failover to the standby switch. **Scenario:** On rebooting the master switch, the AP sends a failover request to the standby switch before the Heart-beat Timer (HBT) threshold. By this time, the standby switch is in BACKUP mode and it rejects the failover request from the AP. By the time, the standby switch becomes active, the AP fails to retransmit the failover request to the standby switch (currently the active/master switch). As a result, the AP does not failover to the standby switch. This issue is observed in switches running AOS-W 6.4.4.x or AOS-W 6.5.x. **Workaround:** None.	HA-Lite	All platforms	AOS-W 6.5.0.0
149594	**Symptom: AMON_USER_INFO_MESSAGE** does not contain the user-agent info, whereas the SNMP user info has the user-agent information. **Scenario:** This issue is observed in a master-local setup when choosing AMON over SNMP in OV3600 This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** Choose SNMP in OV3600.	Base OS Security	All platforms	AOS-W 6.4.3.9

Upgrade Procedure

This chapter details the software upgrade procedures. Alcatel-Lucent best practices recommend that you schedule a maintenance window for upgrading your switches.

CAUTION

Read all the information in this chapter before upgrading your switch.

Topics in this chapter include:

- Upgrade Caveats on page 61
- GRE Tunnel-Type Requirements on page 62
- Important Points to Remember and Best Practices on page 62
- Memory Requirements on page 63
- Backing up Critical Data on page 64
- Upgrading in a Multiswitch Network on page 65
- Installing the FIPS Version of AOS-W 6.5.1.0 on page 65
- Upgrading to AOS-W 6.5.1.0 on page 66
- Downgrading on page 69
- Before You Call Technical Support on page 71

Upgrade Caveats

- OAW-AP120 Series access points, OAW-4306 Series, OAW-4x04 Series, OAW-S3, and OAW-6000 switches are not supported from AOS-W 6.5.x. Do not upgrade to AOS-W 6.5.x if your deployment contains a mix of these switches in a master-local setup.
- If your switch is running AOS-W 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the AOS-W image to the nonboot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from AOS-W 6.4.x, you cannot create redundant firewall rules in a single ACL. AOS-W will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

If you are upgrading from AOS-W 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the following ACL, both ACE entries could not be configured in AOS-W 6.4.x. When the second ACE is added, it overwrites the first.

```
(host)(config) #ip access-list session allowall-laptop
(host)(config-sess-allowall-laptop) #any any any permit time-range test_range
(host)(config-sess-allowall-laptop) #any any any deny
(host)(config-sess-allowall-laptop) #!
(host)(config) #end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority        Source  Destination     Service Action  TimeRange
--------        ------  -----------     ------- ------  ---------
1               any     any             any     deny
```

- When upgrading the software in a multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 65.)

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel with respect to tunnel type:

- AOS-W 6.5.1.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each switch? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?

  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the switch. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *AOS-W 6.5.x User Guide*.

Memory Requirements

All Alcatel-Lucent switches store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the switch. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 60 MB of free memory available for an upgrade using the WebUI, or execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI. Do not proceed unless this much free memory is available. To recover memory, reboot the switch. After the switch comes up, upgrade immediately.
- Confirm that there is at least 75 MB of flash space available for an upgrade using the WebUI, or execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI.

CAUTION

In certain situations, a reboot or a shutdown could cause the switch to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any switch logs, crash data, or flash backups should be copied to a location off the switch, then deleted from the switch to free up flash space. You can delete the following files from the switch to free up some memory before upgrading:

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 64 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 64 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the switch.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 64 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- X.509 certificates
- Switch Logs

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the switch:

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the switch's command line:

1. Make sure you are in the **enable** mode in the switch CLI, and execute the following command:

```
(host) # write memory
```

2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

```
(host) # backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
```

```
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```

4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

   ```
   (host) # restore flash
   ```

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 64.

NOTE

For proper operation, all switches in the network must be upgraded with the same version of AOS-W software. For redundant environments such as VRRP, the switches should be of the same model.

To upgrade an existing multiswitch system to this version of AOS-W:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the switches. Reboot the master switch. After the master switch completes rebooting, you can reboot the local switches simultaneously.
   b. Verify that the master and all local switches are upgraded properly.

Installing the FIPS Version of AOS-W 6.5.1.0

Download the FIPS version of the software from https://service.esd.alcatel-lucent.com.

Instructions on Installing FIPS Software

NOTE

Before you install a FIPS version of the software on a switch that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the switch, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

Follow the steps below to install the FIPS software on a switch that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the switch.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the switch using the CLI or WebUI.
3. Reboot the switch by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

Upgrading to AOS-W 6.5.1.0

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.1.0 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 63.

NOTE

When you navigate to the **Configuration** tab of the switch's WebUI, the switch may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade the switch from the WebUI and navigate to the **Configuration** tab as soon as the switch completes rebooting. This error is expected and disappears after clearing the Web browser cache.

NOTE

When upgrading from an existing AOS-W 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.4.3.9.

Install the AOS-W software image from a PC or workstation using the WebUI on the switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download AOS-W 6.5.1.0 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

The AOS-W image file is digitally signed, and is verified using RSA2048 certificates preloaded on the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch will not load a corrupted image.

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the switch to reboot immediately.

NOTE

Upgrade will not take effect until you reboot the switch.

9. Choose **Yes** in the **Save Current Configuration Before Reboot** radio button.
10. Click **Upgrade**.

    When the software image is uploaded to the switch, a popup window displays the **Changes were written to flash successfully** message.
11. Click **OK**.

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 64 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

Install Using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 63.

To install the AOS-W software image from a PC or workstation using the CLI on the switch:

1. Download AOS-W 6.5.1.0 from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.

   ```
   (host)# ping <ftphost>
   ```

   or

   ```
   (host)# ping <tftphost>
   ```

   or

   ```
   (host)# ping <scphost>
   ```

4. Execute the **show image version** command to check if the AOS-W images are loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.
5. Execute the **copy** command to load the new image onto the nonboot partition.

   ```
   (host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
   ```

NOTE

The USB option is available on the OAW-40xx Series and OAW-4x50 Series switches.

6. Execute the **show image version** command to verify that the new image is loaded.
7. Reboot the switch.

   ```
   (host)# reload
   ```

8. Execute the **show version** command to verify that the upgrade is complete.

   ```
   (host)# show version
   ```

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.

5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 64 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of AOS-W.

CAUTION

If you upgraded from AOS-W 3.3.x to AOS-W 5.0, the upgrade script encrypts the internal database. New entries created in AOS-W 6.5.1.0 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

CAUTION

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.5.1.0 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group

CAUTION

When reverting the switch software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the switch with the preupgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 64.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.1.0 configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next switch reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W 6.5.1.0 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.1.0 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.5.1.0, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.5.1.0, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the switch to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

   or

```
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the switch to boot with your preupgrade configuration file.

```
(host) # boot config-file   <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.1.0 image.

4. Set the backup system partition as the new boot partition.

   ```
   (host) # boot system partition 1
   ```

5. Reboot the switch.

   ```
   (host) # reload
   ```

6. When the boot process is complete, verify that the switch is using the correct software.

   ```
   (host) # show image version
   ```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Alcatel-Lucent switch with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the switch at the time of the problem. Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the switch.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent switch) or any recent changes to your switch and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the switch site access information, if possible.

Appendix A
Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALG	Application Level Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusuin Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
TPC	Transmit Power Control

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning